



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/807,295	07/13/2001	Yoshiaki Nakanishi	NAKANISHI 2	6043
1444	7590	09/22/2004	EXAMINER	
BROWDY AND NEIMARK, P.L.L.C.			SON, LINH L D	
624 NINTH STREET, NW				
SUITE 300			ART UNIT	PAPER NUMBER
WASHINGTON, DC 20001-5303			2135	

DATE MAILED: 09/22/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

<p align="center">Office Action Summary</p>	<p>Application No</p> <p>09/807,295</p>	<p>Applicant(s)</p> <p>NAKANISHI ET AL.</p>	
	<p>Examiner</p> <p>Linh Son</p>	<p>Art Unit</p> <p>2135</p>	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 13 July 2001.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-44 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-44 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date <u>6</u> . | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Claim Objections

1. Claims 13-16, 18-21, 24-26, 28, and 35-44 are objected to under 37 CFR 1.75(c) as being in improper form because these claims are depending back to another Multiple Dependent claims. See MPEP § 608.01(n).
2. The Claims are objected to because of the following informalities: multiple misspelling words and incorrect spacing between words are found in the claims. There are multiple incorrect spacing between words are found through out the claims, for instance "saidbackup" in claim 21. Appropriate correction is required.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.
4. **Claims 1-10, 14-30, and 35-43 are rejected under 35 U.S.C. 103(a) as being unpatentable over Paltenghe et al, US Patent No. 20020004783A1, hereinafter '783.**

5. As per claims 1-2, and 27, "An electronic information backup system, comprising: electronic wallet means for management of electronic value information, electronic safe means for generating and issuing by accepting registration of an registration certificate electronic value information and extracting the corresponding electronic value information through presentation said registration certificate" is taught in **'783** (Para 0060, 0051, and 0064) [the electronic value is registered to the certificate which is used to authenticate the electronic value]. "Electronic safe storage means that the intrinsic storage area of the electronic safe means for holding said electronic value information corresponding to said registration certificate" is taught in **'783** (Para 0053, 0004, 0006, and 0009) [The Virtual wallet serves as the safe for registered info]. And "said electronic information recovery means acquires the corresponding electronic value information by presenting said registration certificate obtained from said electronic wallet means to said electronic safe means to recover said information on said electronic wallet means" is taught in **'783** (Para 0046). However, **'783** does not specifically explain the registration process of the electronic value information as a whole or partial to the virtual safe to obtain the certificate. Nevertheless, **'783s** teaches that a certificate to access the electronic value located on a remote server. The electronic value located on the remote server is the backup mechanism of the electronic wallet information on the smart card. To access the electronic information, the certificate is needed to authenticate the information on the virtual wallet (Para 0045-0046, 0064, 0066, and 0067).

Therefore, it would have been obvious at the time of the invention was made for one having ordinary skill in the art that the registration process to link the certificate to the electronic value on the server is implemented in the invention and the linking mechanism must be included a pointer to the remote server to access the correct electronic value info. With such linking mechanism can be implemented to register the electronic value info to multiple servers for high access availability.

6. As per claim 3, claim 1 is incorporated. However, "generating a registration certificate including the own pointer information with said electronic safe means" is not clearly explained in '783. Nevertheless, it is obvious at the time of the invention was made for one having ordinary skill in the art to realize that the own pointer information must exist in order to store the information and be able to retrieve it.
7. As per claim 4, an electronic information backup system according to any one of the claims 1 to 3, "comprising a key storage means for storing a set of an encryption key and a decoding key and an encrypting/decoding means for executing the encryption of said electronic value information using the encryption key and also executing the decoding using said decoding key, wherein said electronic information registration means registers the encryption electronic value

information obtaining by encrypting the electronic value information obtained from said electronic wallet means with said encrypting/decoding means said electronic safe means in order to obtain the encryption electronic value information registration certificate" is taught in **'783** (Para 0078-0080). "And said electronic information recovery means obtains the corresponding encryption electronic value information by presenting said encryption electronic value information registration certificate to said electronic safe means and also obtains said electronic value information decoded with said encrypting/decoding means and then recovers such information on said electronic safe means" is taught in **'783** (Para 0046, and 0078-0080).

8. As per claims 5 and 6, an electronic information backup system according claim 4, "wherein said electronic information registration means acquires a key registration certificate by obtaining a key information from said key storage means" is taught in **'783** (Para 0078-79) [the certificate in the invention is the index itself and the key storage is the key directory]. And "registering this information to said electronic safe means and said electronic information recovery means acquires the corresponding key information by presenting said key registration certificate to said electronic safe means and then recovering said obtained key information on said key storage means" is taught in **'783** (Para 0080) [The key index can be used to recover the public/private key pairs. The public key is encryption key and the private key is the decryption key.].

9. As per claims 7-9, an electronic information backup system according to claim 4, “comprising an electronic information dividing means for dividing said electronic value information to the desired number of partial electronic information pieces to which an identifier for recovering said electronic value information to the original electronic value information is respectively added and an electronic information combining means for recovering said original electronic value information from said divided electronic information pieces, wherein said electronic acquires a plurality of partial by requesting division of said electronic value information to said electronic information dividing means and also acquires information registration means electronic information pieces respective partial information registration certificates registering the entire part or a part of said partial electronic information to the electronic safe means, said electronic information recovery means acquires respective corresponding partial electronic information pieces by presenting the entire part or a part of said partial information registration certificates to the electronic safe means that has issued the respective partial information registration certificates, and said electronic information combining means recovers said electronic value information from said obtained partial electronic information pieces” is not clearly teach in **‘783** . Nevertheless, **‘783** teaches the certificate link to plurality of the electronic value info, which the applicant named information pieces. The electronic value info comprises of the listing in Para 0051, which is stored in a database for retrieval

when needed. The linking mechanism must exist in order to retrieve the electronic value info from the database (Para 0045, 0051, 0060, and 0046).

Therefore, it would have been obvious at the time of the invention was made for one of ordinary skill in the art that **'783** does includes the feature claimed above to be able to store the pieces of information and to retrieve the electronic value information when a transaction is carried out.

10. As per claim 10, this claim incorporates substantially similar subject matter as in claims 7, and is rejected along the same rationale. However, the coupling and decoupling means are not specifically taught by **'783**. Nevertheless, **'783** teaches the certificate links all pieces of electronic information values together and the certificate is the mechanism used to get access to any or all of the electronic information values (Para 0006, 0014, 0045-46, 0079, and 0088). Therefore, it is obvious for one having ordinary skill in the art at the time of the invention was made that the coupling and decoupling means exist in order to retrieve the desired electronic information value for a certain electronic transaction.

11. As per claim 14, **"an electronic information backup system comprising an owner information input means for inputting the intrinsic owner information and an owner authentication information input means for inputting the**

corresponding owner authentication information to said owner information, wherein said electronic information registration means registers a set of said electronic value information and the owner authentication information obtained from said owner authentication information input means to said electronic safe means and said electronic information recovery means can acquire said electronic value information when collation with said owner authentication information presenting the owner information input" is taught by '783 (Para 0009, 0046, and 0051).

1. As per claims 15, 19, 37-40, and 42, "an electronic information backup system comprising completed successfully by information obtained from said owner means to said electronic safe means an owner information input means for inputting the intrinsic owner information, an owner authentication information storage means for holding the owner authentication information corresponding to said owner information and an owner authentication means for inspecting said owner information with said owner legitimacy by comparing authentication information, wherein authentication is performed by presenting the owner information inputted from said owner information input means to said owner authentication means, forming an encryption communication path between said electronic information registration means and electronic safe means using the authentication result, said electronic information registration means

registers said electronic value information to the electronic value information through said encryption communication path, said electronic safe means holds a set of the owner authentication information corresponding to said authentication result and said electronic value information to the electronic safe means and said electronic information recovery means acquires, path, said electronic through said encryption communication value information corresponding to said owner authentication information corresponding to said authentication result" is taught by '783 (Para 0009, 0046, 0051, and 0054).

2. As per claims 16 and 17, an electronic information backup system according to claims 6 and 15, **"wherein said owner information input means and owner authentication means generate a common key to use temporarily and hold in common and thereafter encrypt the owner information with said common key to send the encrypted owner information to the owner authentication means"** is not taught by **'783** specially. However, **'783** does teach a secure communication link from the user to the storage implemented to transfer personal information and other type of transactions with the storage server (Para 0052, and 0054). Therefore, it would have been obvious at the time of the invention was made for one having ordinary skill in the art that the common key for temporarily used is explicitly taught in **'783** to provide a secure communication between the client and the storage server.

3. As per claim 18, **“an electronic information backup system comprising an authentication device read means for reading an authentication device used for the owner authentication an authentication check means for inspecting legitimacy of said authentication device and an authentication check information storage means for storing the information to be compared for checking legitimacy of said authentication device with said authentication check means whereby the authentication device connected said authentication device read means and the authentication check means mutually check the legitimacy”** is taught by **‘783** in (Para 0046) [the authentication process must exist in order to open the virtual wallet for access].
4. As per claim 20, **“An electronic information backup system comprising a backup condition storage means for storing the condition information for backup of the electronic value information and a backup object extraction means for selecting the backup object from said electronic wallet means by interpreting the backup condition obtained from said backup condition storage means, wherein said electronic information acquires the corresponding registration automatically registering of backup object said electronic safe means”** is taught by **‘783** in (Para 0046, and 0053) [The backup condition storage means is to ensure the high availability of the electronic wallet and to be able to recover when necessary].

5. As per claim 21, this claim incorporates substantially similar subject matter as in claim 20, and is rejected along the same rationale. **Further “a vacant capacity is expanded by deleting said electronic value information as the backup object from said electronic wallet storage means, and when the sufficient vacant capacity is reserved, the electronic information is recovered on said electronic wallet means or a new electronic value information is registered”** is not taught by ‘783. However, ‘783 teach the storage capability to create a high availability and secure environment for the electronic value information. A part of the high availability storage environment must ensure a storage space for user to register new electronic value information (Para 0046). Therefore, it would have been obvious at the time of the invention was made for one of ordinary skill in the art that the vacant capacity reservation is explicitly taught by ‘783 in order to ensure a high availability storage environment for the new electronic values registration.
6. As per claim 22, An electronic information backup system according to claim 6, **“wherein when the owner authentication to the other electronic safe means registering said decoding key is completed successfully, said other electronic safe means acquires the encryption electronic information through the communication with the electronic safe means having registered the electronic value information other than said decoding key**

and said electronic information recovery means acquires said encrypted electronic value information from the other electronic safe means and then recovers such electronic value information on said electronic wallet means" is taught by **'783** in (Para 0046, 0066-67, and 0095) [The key is used to authenticate to the storage and the certificate has linking mechanism to all the electronic information values which can be used to recover the lost electronic information values back on to the electronic wallet].

7. As per claim 23, **'783** teaches **"An electronic information backup system according to claim 6, wherein when owner authentication to the other electronic safe means registering said decoding key is completed successfully, said other electronic safe means acquires the encryption electronic information by making communication with the electronic safe means registering the electronic value information other than said decoding key"** is taught in (Para 0046 and 54). **"said electronic information recovery means acquires said encrypted electronic value information from said other electronic safe means to recover such information on said electronic wallet means"** is taught by **'783** in (Para 0046) [recovering means by presenting the certificate to get the electronic value information back to the local wallet]. However, **'783** does not teach **"said encrypting/decoding means generates a pair of new encryption key and decoding key, and said electronic value information is encrypted using said new encryption key**

and said new encryption key is sent to said other electronic safe means”.

Nevertheless, **‘783** does teach the capability of generating the public/private key pair by the local user (Para 0078). Therefore, it would have been obvious at the time of the invention was made for one having ordinary skill in the art to modify the invention so that a new pair key can be regenerated after the electronic values got recovered. This feature would prevent the new recovered electronic values to be compromised in the event that someone acquires the previous keys.

8. As per claim 24, an electronic information backup system, “wherein if sufficient capacity for information recovery is not remained on the electronic wallet means when said electronic information recovery means presents the registration certificate to recover the corresponding electronic value information on the electronic wallet means or registers a new electronic value information on the electronic wallet means, shortage of capacity is presented to a user to suspend the recovery job” is not specifically taught by **‘783**. However, it would have been obvious at the time of the invention was made for one having ordinary skill in the art that such a safety mechanism is in place in the event of storage capacity shortage must be implemented by default.
9. As per claim 25, **‘783** does not teach “the said electronic information registration means acquires the corresponding registration certificate by registering the electronic value information obtained from said electronic wallet means to said

electronic safe means and deletes, when said registration certificate is normally registered to said electronic wallet means, said electronic value information from said electronic wallet means". However, **'783** does teach the utilization of the certificate to access the electronic values locating in registered wallet locating on the server for any particular transaction. For such application utilizing the certificate, the electronic value information on the local electronic wallet is no long necessary (Para 0045-46). Therefore, it would have been obvious at the time of the invention was made for one of ordinary skill in the art that the electronic value information is not necessary to be on the local electronic wallet. For that reason, the electronic value can be deleted from the local electronic wallet and make space for new electronic value information registration.

10. As per claims 26 and 35, "an electronic information backup system wherein said electronic information recovery means acquires the corresponding electronic value information from said electronic safe means by presenting the registration certificate obtained from said electronic wallet means and deletes, when said electronic value information is normally recovered on the electronic wallet means said registration certificate from said electronic wallet means" is taught by **'783** in (Para 0046). However, "deleting said electronic value information from said electronic safe means when the electronic value information is normally recovered on the electronic wallet" is not specifically taught by **'783**. Nevertheless, **'783** teaches the electronic wallet content locating in both the

remote safe storage and the local electronic wallet (Para 0045). Further **'783** also includes a backup storage party (Para 0053) to ensure the electronic value data is lost in both locale electronic and the virtual wallet. Therefore, it would have been obvious at the time of the invention was made for one having ordinary skill in the art that removing the electronic value information from the electronic safe will not cause the high availability electronic wallet disable in the event of catastrophe since the data can be recovered at ease from either the local electronic wallet or on the backup storage party.

11. As per claim 28, "an electronic information backup system, wherein said registration certificate includes partial information of the electronic value information" is taught by **'783** in (Para 0046).
12. As per claim 29, "an electronic information backup systems comprising backup means for acquiring an encryption electronic value information by encrypting the electronic value information requested for registration using an encryption key and said encryption electronic value information is then registered to external server" is taught by **'783** in (Para 0064) [The encryption key is also the certificate and is utilized to encrypt the electronic value information].
13. As per claim 30, "an electronic information backup systems comprising backup means for acquiring the corresponding encryption electronic value information by

presenting the registration certificate requested for recovery to the external server and recovers said encryption electronic value information to the electronic value information using the decoding key” is taught by ‘783 in (Para 0046 and 0064).

14. As per claim 36, ‘783 teaches “An electronic information backup system”. However, ‘783 does not specifically teach “ wherein the electronic value any one information as the backup object is selected from said storage medium by interpreting the preset backup condition and said selected electronic value information is automatically registered to said external server to acquires the corresponding registration certificate”. Nevertheless, ‘783 does teach the updating process of the electronic values from the local electronic wallet to the virtual wallet located on the external server (Para 0047 starting at the 4th sentences down). The updating process will register any specific electronic value contains in the wallet. Therefore, it would have been obvious at the time of the invention was made for one having ordinary skill in the art that the updating process in ‘783 includes the registration process of the electronic value information in order for the user to access the information.
15. As per claim 41, “**An electronic information backup system according to any one of claim information is wherein said electronic value acquired when an IC card recording the owner authentication information is read, such**

authentication information is sent to the external server and said external server checks legitimacy of said authentication information is taught by **'783** in (Fig. 1, Para 0046, and 0054).

16. As per claim 43, "An electronic information backup system, wherein when the owner authentication to the other external server registering the decoding key is completed successfully, said other external server makes communication with the external server registering the electronic value information other than said decoding key information and acquire the encryption electronic encryption electronic information is coupled with said decoding key" is taught by **'783** in (Para 0046, and 0053-54) [The decoding key is corresponding to the certificate and uses to access the virtual wallet].
17. **Claims 11-12, 31-34, and 44 are rejected under 35 U.S.C. 103(a) as being unpatentable over Paltenghe et al, US Patent No. 20020004783A1, hereinafter '783, in view of Cordery, US Patent No. 6738899B1, hereinafter '899.**
18. As per claims 11 and 33-34, "**An electronic information backup system according to claim 10**" is taught by **'783**. However, **'783** does not teach "**wherein said electronic information dividing means divides the key information obtained by said electronic information registration means**

from said key storage means into plurality of partial keys said
encrypting/decoding means acquires the encryption electronic information
by encrypting the electronic value information obtained by said electronic
information registration means from said electronic wallet means, said
electronic information coupling means acquires the coupled electronic
information from said encryption electronic information and the partial key
group A as a part of said partial key: said electronic information
registration means acquires the corresponding registration certificate by
registering said coupled electronic information and the partial key group B
as the remaining partial key to different electronic safe means respectively,
said electronic information recovery means acquires said coupled
electronic information and said partial key group B by presenting said
registration certificate to the corresponding electronic safe means said
electronic information decoupling means isolates said coupled electronic
information to said encryption electronic information and said partial key
group A, said electronic information combining means combines said
partial key group A and said partial key group A to generate a key
information, said encrypting/decoding means decodes said encryption
electronic information and acquires said electronic value information, and
said electronic information recovery means acquires said key information
to recover this information on said recovers said electronic value wallet
means". Nevertheless, '899 does teach a public key encryption system in which

a user registers a certificate at multiple certificate authority (CA). In the system, the public data storage stores the user's corresponding encryption/decryption key of the certificate for every CA's and the user certificate (Col 7 lines 22-59).

Analogously, the each CA is comparing to the divided piece of electronic information, and all these pieces of electronic information partial keys are stored in the public storage associated to a user or a group. The recovery process is the summation of all the keys explained clearly in (Col 8 lines 15-25). The decoupling is the process of separating the pieces of electronic information to register at different CA. Therefore, it would have been obvious at the time of the invention was made for one having ordinary skill in the art to combine '899 with '783 to create a more secure and organize key directory in order to retrieve the information conveniently.

19. As per claim 12, **"An electronic information backup system according to claim 11"** is taught by '783 and '899. **"wherein said electronic information dividing means sets the partial key obtained by dividing the key information the original information to generate a pair of keys of the encryption key and the decoding key"** is taught by '899 in (Col 8 lines 48-55).
20. As per claims 31 and 32, '783 does not teach **"an electronic information backup system, comprising a backup means that acquires a plurality of partial electronic information pieces by dividing the electronic value**

information requested for registration, also acquires the partial information registration certificates in the same number as said partial electronic information pieces by registering partial electronic information pieces to the desired number of external servers and also stores all partial information registration certificates to a storage memory". Nevertheless, '899 does disclose an encryption/decryption system using the registration certificate registered at plurality of certificate authority (CA). The certificates and the keys are stored at the public data storage corresponding to the user. Analogously, the registered certificates at plurality of CA are linking to the divided pieces of electronic information. To recover the data, all certificates and keys corresponding to the user stored in the public data storage can be summed to recover the certificate, which associates to all the electronic information. Therefore, it would have been obvious at the time of the invention was made for one having ordinary skill in the art to implement '899's teaching to modify the invention for security and data organization purpose. Each CA can provide different services for the user relating to the stored information.

21. As per claim 44, claim 11 is incorporated. In addition, "the encryption electronic information is registered to said external server and simultaneously the decoding key is registered to the other external server" is taught by '899 in (Col 7 lines 22-58) [the external server storing the keys is the public data store (Fig 7, # 46).

22. **Claims 13 is rejected under 35 U.S.C. 103(a) as being unpatentable over Paltenghe et al, US Patent No. 20020004783A1, hereinafter '783, in view of Gennaro et al, US Patent No. 5937066, hereinafter '066.**
23. As per claim 13, **'783** teaches "An electronic information backup system and an electronic wallet that contains certificate info which can remotely access the electronic value information located on an external server". However, **'783** does not teach "comprising an original encryption seed information used to generate the decoding key and a decoding key generation algorithm to generate the decoding key from said encryption seed information, wherein said electronic information registering means acquires the corresponding encryption seed information registration certificate by registering said encryption seed information said electronic safe means said electronic information recovery means acquires the corresponding encryption seed information from said electronic safe means by presenting said encryption seed information registration certificate, said encrypting/decoding means generates the decoding key by multiplying said encryption said information said decoding key generation algorithm and said electronic information recovery means decodes said electronic value information obtained by said electronic information recovery means using said decoding key". Nevertheless, **'066** teaches a method of generating and recovering an encryption/decryption key using secret information (seed) in (Col 10 line 51 to Col 10 line 11). Therefore, it would have been obvious at the time of the

invention was made for one having ordinary skill in the art to combine the key generation/recovery method of '066 with '783 to provide a mechanism to protect the encryption key and the encrypted data using the key.

Conclusion

24. Any inquiry concerning this communication from the examiner should be directed to Linh Son whose telephone number is (703)-305-8914.
25. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor Kim Y. Vu can be reached at (703)-305-4393. The fax numbers for this group are (703)-872-9306 (official fax). Any inquiry of general nature or relating to the status of this application or proceeding should be directed to the group receptionist whose telephone number is (703)-305-9600.
26. **Please notice.** Due to the Office moving, the telephone numbers above will only be valid until October 15th of 2004. After that, the following list of numbers will be valid:

Examiner: (571) 272-3856.

Kim Y. Vu: (571) 272-3859

Receptionist: (571) 272-2100

Application/Control Number: 09/807,295

Page 23

Art Unit: 2135

Linh LD Son

Patent Examiner

Handwritten signature
Au 2135